ABSTRACT

A system in accordance with an embodiment of the invention includes a vulnerability detection system (VDS) and an intrusion detection system (IDS). The intrusion detection system leverages off of information gathered about a network, such as vulnerabilities, so that it only examines and alerts the user to potential intrusions that could actually affect the particular network. In addition both the VDS and IDS use rules in performing their respective analyses that are query-based and that are easy to construct. In particular these rules are based on a set of templates, which represent various entities or processes on the network.